The L Suite
LegalOps

AI Governance Checklist

Safeguard Accuracy and Reduce Risk in AI-Assisted Legal Work

AI is now embedded in how many legal teams work, accelerating drafting, research, and review. But without oversight, it can also introduce serious errors, from fabricated citations to confidentiality breaches.

Legal Operations is best positioned to prevent those mistakes by defining the systems, workflows, and guardrails that keep AI reliable and compliant. Use these checklists to help your department adopt AI with confidence and control.

1. AI Policy & Workflow

Set clear policies and processes to guide AI use responsibly.

- □ Define acceptable AI use cases (e.g., research, drafting, summarization).
- □ Build a cross-functional AI policy with Legal, IT, InfoSec, and Compliance that protects the company while encouraging responsible use.
- □ Maintain a vetted list of approved tools reviewed by Legal Ops and Compliance.
- □ Document AI use in matter management or workflow systems.
- □ Monitor and restrict unapproved or “shadow” AI tools to prevent untracked data exposure.
- □ Add a simple way to tag or track AI-assisted work in existing systems.
- □ Define escalation triggers for when AI output appears incorrect, biased, or risky.

2. Data Security & Confidentiality

Protect what should never leave your organization.

- □ Prohibit uploading client, employee, or internal data into public AI tools.
- □ Provide an explicit “never upload” list (e.g., privileged documents, internal investigations, M&A materials, export-controlled data).
- □ If appropriate, redact identifying information before uploading any text or document.
- □ Review each tool’s data retention and privacy practices during approval.
- □ Train teams to avoid entering confidential or privileged details in prompts.
- □ Offer approved prompt patterns for sensitive work such as contract summaries, redlines, or risk assessments.

3. Accuracy & Quality Control

Trust the tool but verify the output.

- □ Cross-check all AI-generated citations, quotes, and legal references.
- □ Define mandatory human review points inside key workflows for filings, contracts, and other high-risk materials.
- □ Run test sets before using new AI workflows at scale to establish expected accuracy and variance.
- □ Test approved AI tools internally with the legal team before rolling them out to business users or clients.
- □ Validate the accuracy of AI outputs against known examples, benchmarks, or prior matters.
- □ Re-test tools periodically as vendors release new models or major feature updates.
- □ Track and flag inaccuracies to improve future prompts or training.
- □ Create an easy path for users to report incorrect or concerning outputs.

AI Governance Checklist

4. Compliance & Consent

Use AI notetakers and recording tools responsibly.

- □ Get consent before using AI notetakers in meetings or interviews.
- □ Provide a standard consent script for meetings when AI notetakers are used.
- □ Ensure any recording tools are approved for security and data handling.
- □ Exclude privileged or investigatory discussions from recordings.
- □ Set default exclusions for AI notetakers (e.g., privileged meetings, investigations, outside counsel strategy sessions).
- □ Stay current on evolving consent and privacy requirements.

5. Training & Culture

Build awareness, confidence, and accountability around AI use.

- □ Add AI awareness to onboarding and ongoing training.
- □ Deliver role-specific training tailored to attorneys, contracting teams, paralegals, and business users.
- □ Provide refreshers as capabilities evolve.
- □ Create feedback loops so users can flag issues or suggest improvements.
- □ Monitor usage patterns and analytics from enterprise AI tools to spot risks, training needs, or adoption gaps.
- □ Reinforce that AI assists judgment and doesn't replace it.
- □ Publish prompt libraries or templates in the systems where work happens (CLM, knowledge base, Teams/Slack).
- □ Identify AI champions within Legal and the business to reinforce best practices.

6. Platform Oversight

Close any gaps as AI rolls out to enterprise systems.

- □ Establish a defined review path for new AI tools, including approval criteria, required risk inputs, and evaluation timelines.
- □ Clarify rules for platform-native AI tools (e.g., Microsoft, Google, CLM-embedded AI) to distinguish them from public AI tools.
- □ Require review of AI features embedded in legal technology platforms before enabling them.
- □ Determine who can enable or disable new AI capabilities in enterprise platforms.
- □ Create requirements for reviewing model changes or new feature rollouts.
- □ Establish access, offboarding, data retention, and audit expectations for AI-enabled tools.
- □ Create a cadence for re-evaluating platform AI features as vendors update them.

Final Check

Before using AI for any legal task, ask:

- ☑ Does this workflow need adjustment before using AI?
- ☑ Is this tool approved and secure?
- ☑ Is the data appropriate to share?
- ☑ Have I verified accuracy?
- ☑ Would I stand behind this output if it reached a client or the business?

If the answer to any is "no," pause and review before proceeding.

Next Step

Legal Ops leaders are defining how AI transforms the legal department. Join The L Suite to see how peers are comparing policies, building frameworks, and sharing what works in practice.

Join The L Suite Community →